kasada

Quarterly Threat Report

Q1 2024

Table of Contents

Welcome to Kasada's Quarterly Threat Report

Welcome to the Q1 2024 edition of the Kasada Quarterly Threat Report, where we share the latest insights and data on the evolving landscape of automated threats and online fraud.

In this edition, we provide an overview of the top trends and adversary activities observed from January through March 2024. Our report includes comparisons with data from previous quarters, leveraging both internal research and external investigations to deliver a holistic view of the automated attack ecosystem.

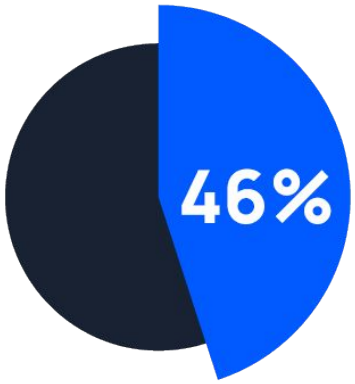
The primary goal of the Quarterly Threat Report is to equip cybersecurity and threat intelligence professionals with the critical information needed to understand and counteract current attack vectors. By sharing knowledge and proven strategies, Kasada aims to foster collaboration and strengthen the security resilience of organizations worldwide.

Our unmatched insights into the tactics and motivations of cyber adversaries empower security and technology teams to make informed decisions, enhance their detection capabilities, and proactively mitigate emerging threats.

Q1 2024 Attack Trends

Bad Bot vs. Human Traffic

Nearly half (46%) of all web traffic we observed in Q1 2024 was generated by bad bots, highlighting the pervasive nature of automated threats.



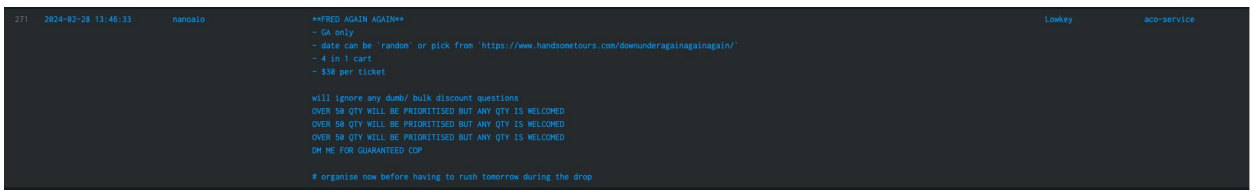
Bad Bot Traffic

Bad bots are automated scripts designed to perform malicious activities across the Internet, unlike good bots that perform helpful functions, such as search engine indexing.

Recognizing this prevalence is key to prioritizing robust bot mitigation strategies to protect your website, applications, and APIs assets from malicious actors.

Attack Techniques and Tactics

Threat actors are constantly evolving their tactics, and this quarter is no different. In Q1 2024, we observed a significant increase in the sophistication and coordination of automated attacks. Adversaries are utilizing a blend of existing and new solver services, along with advanced exploit kits, to bypass traditional bot mitigation tools effectively. This evolution demonstrates a strategic shift towards more organized and financially motivated online fraud activities.



Attack Techniques and Tactics (Continued)

Key Observations

1. Advanced Solver Services:

- **Technique:** Attackers are leveraging solver services that can automatically bypass CAPTCHA and other human verification methods. These services use machine learning algorithms and human-assisted solutions to mimic legitimate human interactions.
- **Impact:** This allows bots to seamlessly navigate through security checks, making it difficult for traditional defenses to differentiate between human and bot traffic.

2. Exploit Kits:

- **Technique:** New and updated exploit kits are being deployed to target vulnerabilities in web applications, APIs, and third-party integrations. These kits are designed to automate the exploitation process, enabling attackers to launch large-scale attacks with minimal effort.
- **Impact:** The use of exploit kits increases the efficiency and scalability of attacks, posing a significant threat to organizations that rely on legacy security measures.

3. Masquerading as Legitimate Traffic:

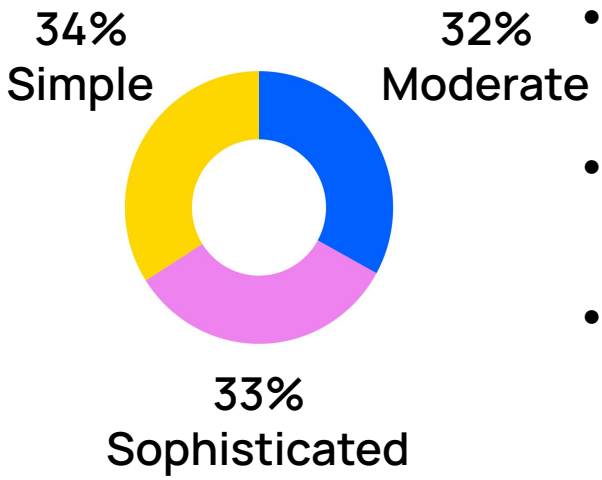
- **Technique:** Coordinated bot attacks are increasingly sophisticated, with bots designed to mimic legitimate human behaviour. These bots can simulate mouse movements, keystrokes, and other user interactions to evade detection.
- **Impact:** This tactic not only complicates detection efforts but also indicates a shift towards using bots for organized online fraud.

4. Underground Forum Discussions:

- **Insight:** Our monitoring of underground forums has revealed ongoing discussions about upcoming account takeover campaigns and arbitrage opportunities. These forums are hotbeds for the sale of automated tools and services that facilitate these activities.
- **Impact:** The accessibility and affordability of these tools lower the barrier to entry for bad actors, leading to an increase in the frequency and scale of automated attacks.

Bad Bot Sophistication Levels

Sophisticated bots, comprising one-third (33%) of observed activity, are employing advanced evasion techniques to bypass traditional detection mechanisms.



- **Simple:** 34% of bots used simple techniques and basic tools, such as fake Google bots or cURL commands.
- **Moderate:** 32% of bot used mid-level sophistication techniques and tools, such as fake browser attacks.
- **Sophisticated:** 33% of bots used highly sophisticated techniques and tools, such as Google Puppeteer and Microsoft Playwright.

Being aware of adversaries' level of sophistication enables you to adapt your defense strategies accordingly.

Geographical Breakdown

Analysis of bot activities reveals hotspots in regions with high adversarial activity, including the United States, Great Britain, Japan, Australia, and China.

Industry-Specific Threat Landscape

Overview

The Kasada Threat Intelligence team continually monitors and assesses early warning signs of automated attacks and online fraud. A key indicator of account fraud is the trade of stolen accounts, which we analyze across various industry sectors. These accounts are typically obtained through info-stealing malware, data breaches, and brute-force attacks using tools such as OpenBullet.

The following industry-specific analysis focuses on the impact and characteristics of the threat landscape observed in recent quarters, particularly following a significant credential stuffing attack on a large US email provider reported in our Q3 2024 Quarterly Threat Report.

Market Dynamics

The value of stolen accounts varies based on several factors, including the type of account, the specific victim company, and the features included (e.g. points, payment cards, digital goods). The pricing is influenced by:

- **Rewards points:** Highly valued across multiple industries, as they can be redeemed for bookings, discounts, or transferred to other accounts.
- **Payment card details:** Accounts with valid payment cards command higher prices; often associated with traditional account takeover.
- **Gift card details:** Redeemable for cash value, offering anonymity and ease of use, making them popular to use for fraudulent activities.
- **Access features:** Common in streaming and gaming accounts; valued for their immediate access to premium content and digital goods.

All quoted prices are in USD, reflecting the international nature of the underground markets where these accounts are traded. Prices fluctuate based on the perceived value and demand within the specific verticals.

Airlines

Demand for airline accounts remained low throughout Q1, with sales down over 60% compared to Q4 2023. Notably, over 50% of sales impacted a single European carrier, the same carrier we highlighted in the Q3 2023 Quarterly Threat Intelligence Report.

Despite the overall drop in demand, the average price of each observed sale nearly doubled from Q4 to Q1, rising from just under $13.00 to over $25.00. This price increase was driven by a significant drop in demand for low-value accounts (those with fewer than 50,000 loyalty points for US-based carriers) while demand for high-value accounts (especially for European-based carriers) remained strong.

Available account stock trended upwards over the quarter, finishing Q1 with stock levels approximately 13% higher than Q4. Low demand throughout the first quarter of 2024 has allowed vendors to restock, likely in anticipation of the upcoming northern hemisphere travel season.

Gaming

The value of gaming accounts is determined by the type of content available and any additional features or in-game assets included. Observed sales of gaming accounts continued to be dominated by Steam, PlayStation, and free-to-play games such as Roblox, Valorant, and Fortnite. Total sales over Q1 remained relatively steady, increasing by about 3% when compared to Q4 2024. At the same time, the average cost of each sold account reduced from $1.90 to approximately $1.07, resulting in a revenue reduction of over 40% for account sellers.

A single seller accounted for more than 60% of all gaming account sales. This is likely an inflated metric as the seller does not offer access to each account but rather provides access to the registered email for each account type. The seller provides access to a compromised email account with a linked gaming account, potentially allowing the sale of an identical email account multiple times, once for each associated account.

Other major sellers within the gaming vertical supply “logs”, or unverified username:password combinations likely leaked during data breaches. As these logs are not guaranteed to work, they are sold for incredibly cheap, often as low as $0.01 per account. The increase in sales of email-based accounts and logs accounts for the drop in the average price this quarter.

Hospitality

Accommodation accounts are highly valued for their rewards points, which can be redeemed for bookings or transferred to other accounts. The value of these accounts can spike during travel seasons when demand for accommodations increases.

Observed hospitality account sales followed a similar pattern to those in the retail vertical, consistent but low demand resulted in a noticeably reduced number of sales over Q1. The number of accounts sold reduced by more than half, while the average price dropped from over $9.00 to under $5.00. The reduced average sold price was driven, in part, by a drop in demand for high-end hotel accounts with associated large rewards points values.

The available account stock remained steady throughout the quarter, with negligible difference between the start of Q1 and the end. This indicates that the account sellers have been able to gain access to new stolen accounts, as required, in order to keep availability consistent with demand.

Retail

Retail and eCommerce accounts often include payment card details and rewards points. These accounts are frequently targeted due to their direct financial value, enabling attackers to make unauthorized purchases.

Sales of retail accounts remained consistent and relatively low over Q1, in line with expectations following the holiday season in the previous quarter. Total observed sales were 45% lower than Q4 2023. There were no major spikes of activity during the quarter, apart from two large sales of accounts for a food delivery app in early January and early March. In both cases, the sales were obtained during a single transaction. This is likely to be a single threat actor seeking to commit payment card fraud.

The average price of sold accounts dropped significantly between Q4 and Q1, from $1.51 to $1.15. This is likely due to the drop in demand for retail accounts with high-value payment cards after the 2023 holiday sales.

Available account stock decreased steadily throughout the quarter. Vendors limited their restocking of retail accounts during Q1. Between January 1st and March 16th, stock numbers dropped over 13%, with availability increasing after March 17th due to a single vendor making a large number of cheap, low-quality big box retail accounts available for sale.

Social Networks

Social network accounts are generally sold in bulk and are used for various fraudulent activities, including boosting social media engagement and advertising fraud. The price for these accounts is influenced by their age, activity level, and follower count.

Observed sales of social media accounts continued to increase, up from approximately 175,000 in Q4 to over 260,000 in Q1. Over the same period, the average price continued to drop, down two cents to $0.35. Perhaps unsurprisingly, this trend was again driven by sales of X (formerly Twitter) accounts which increased threefold over Q4 2023. Verified/X Premium accounts continued to be available for purchase for as little as $0.05, while aged (therefore seen as more trustworthy) accounts from 2009 cost $0.99.

Discord accounts also continued to be in high demand, with observed sales doubling over the previous quarter. The average price of a sold account remained steady at about $0.30.

Streaming

Streaming accounts are sought after for their immediate access to premium content. As streaming services continue to crack down on account sharing, the observed demand for stolen streaming accounts continued to drop throughout Q1 2024.

Low-priced accounts without warranty have become less popular, likely due to the chance of purchasers being locked out. This is reflected in the average price of observed sales, which doubled from Q4 to Q1 - $1.89 to $3.78. The majority of the higher-priced account sales include either 6 or 12 month warranty. The seller guarantees to replace the account if the purchaser loses access before the time period expires.

There was a spike of account sales for one particular streaming platform in early February, which correlated with the international broadcast of an in-demand sporting event.

The number of accounts available for purchase remained steady throughout the quarter, with sellers restocking to match ongoing demand.

Methodology

The Kasada Threat Intelligence team leverages proactive approach to uncovering and analyzing information on stolen accounts across various industries.

Our methodology combines deep community embedding, advanced data analytics, and engagement in underground marketplaces to provide actionable insights and early warning signs of new attack vectors and fraud techniques.

Our proprietary service, KasadaIQ for Fraud, leverages over 23 million monthly data points across 2,000 non-traditional sources to provide unparalleled context and uncover threats that traditional monitoring methods often miss.

Key features of KasadaIQ include:

- **Comprehensive data mining and data analysis:** KasadaIQ for Fraud mines intelligence from millions of data points gathered from underground sources, including forums, marketplaces, and chat channels.
- **Identify early warning signs:** By participating in these communities, we gain early insights into planned attacks and novel fraud techniques.
- **Detection of business logic abuse:** Our platform excels at detecting abuse of business logic and customer data, identifying threats that bypass conventional security measures.
- **Purchasing and evaluating stolen credentials:** To assess the scope and impact of stolen accounts, our team actively purchases and evaluates credential sets from criminal marketplaces.
- **Understand adversarial tactics:** Direct observation of adversary behaviour helps us understand their methods and strategies, enabling us to anticipate and mitigate threats effectively.

Conclusion

Understanding the trade of stolen accounts across different industries helps organizations recognize the specific threats they face and prioritize their defensive measures accordingly. By staying informed about the evolving tactics and market dynamics of cyber adversaries, organizations can better protect their brands, customers, and digital assets.

About Threat Intelligence at Kasada

Kasada uses threat intelligence to drive the identification of new and emerging threats, techniques and tactics used by adversaries. This identification, coupled with broad access and analysis of open and closed data sources, allows Kasada to rapidly implement new mitigations or identify alternate methods to reduce the impact of automated threats, bot attacks, and online fraud.

The people we're up against are dynamic, well-resourced, and technically proficient. This evolving field means that Kasada needs to be at the forefront of cybersecurity to provide subject matter expertise relating to the capabilities, development pipeline, and targets of specific actors or groups against their networks.

The goal of threat intelligence within Kasada is to reduce the efficacy of the threat ecosystem by providing complete, accurate, relevant, and timely intelligence to customers.

Have a tip for us or want to learn more? Kasada's Threat Intelligence team can be contacted directly at team-threat-intel@kasada.io.

Follow us on LinkedIn, Facebook, and our X handles **@kasada_io** and **@kasadaiq.**

Request a KasadaIQ Assessment

Get in touch

Visit: www.kasada.io

USA: +1-877-473-5073

Australia: 1300-768-601

kasada